



14 July 2025

Wendy McGuinness
Director, McGuinness Institute Te Hononga Waka
[REDACTED]

45 Pipitea St
PO Box 805
Wellington 6140
Phone: +64 4 495 7200
Fax: +64 4 495 7222
Website: dia.govt.nz

CC:
[REDACTED]

Tēnā koe Wendy

Official Information Act 1982 request OIA2425-1224

Thank you for your email of 13 June 2025 requesting information from the Department of Internal Affairs (the Department) under the Official Information Act 1982 (the Act). Your request is appended to this letter as **Appendix A**.

On 30 June 2025, you were notified that question 6 had been transferred to the Government Communications Security Bureau (GCSB) for response. Additionally questions 14-19 were transferred to the Ministry for Transport. The responsibility for answering the relevant part of question 20 has also been transferred to both GCSB and the Ministry of Transport for response.

Role of the The Government Chief Digital Officer

Paul James is the Secretary for Internal Affairs, and also Government Chief Digital Officer (GCDO). The GCDO is responsible for digital leadership across government agencies. In this response we have referred to the GCDO as the holder of the relevant information.

Response to your request

Where the GCDO does not hold the information requested, it is refused under section 18(g) of the Act as no other single agency would hold this information. Where information is held by individual agencies, you may request information directly from those individual agencies. Information about how to contact these agencies is available at www.justice.govt.nz/about/directory-of-official-information/directory-of-official-information-search-tool.

A: New Zealand Government data located in data centres in New Zealand

- 1. Question: Is all New Zealand Government data stored in New Zealand? What percentage of data is stored here? What percentage of agencies only store their data here.*

Response: GCDO is the Digital System Lead and manages the All of Government Digital Portfolio. GCDO is aware that not all government data is stored in New Zealand; however, does not hold information on how much data each agency stores domestically or the percentage of agencies only storing their data in New Zealand. Storing data in New Zealand is at the discretion of individual agencies.

2. *Question: Is the New Zealand Government storing data in Microsoft's first hyperscale data centre in New Zealand? If yes, roughly what percentage? If no, are there any plans to do so?*

Response: Yes, the New Zealand Government does store data in Microsoft's Public Cloud Data Centre; however, GCDO does not hold information on the percentage. The usage of this Public Cloud Data Centre is at the discretion of individual agencies.

3. *Question: Is the New Zealand Government planning to store data at Amazon's new data centre in Auckland, New Zealand? If yes, roughly what percentage?*

Response: It is likely that government data will be held in Amazon Web Services Public Cloud Data Centre; however, GCDO does not hold information on the percentage. The usage of this Public Cloud Data Centre is at the discretion of individual agencies.

4. *Question: Is the New Zealand Government storing data with the New Zealand company Catalyst Cloud? Note that their website (see [here](#)) states that they are an 'approved cloud provider to the New Zealand Government'. If yes, roughly what percentage of data? If no, are there any plans to do so?*

Response: Yes, the New Zealand Government does store data with Catalyst Cloud; however, GCDO does not hold information on the percentage.

Catalyst Cloud holds an All of Government Cloud Framework Agreement, allowing agencies to procure Public Cloud Services and Professional Services under standardised terms. Storing data with Catalyst Cloud is at the discretion of individual agencies.

5. *Question: Can you provide a list of approved cloud providers to the New Zealand Government?*

Response: A list of suppliers that hold All of Government digital contracts managed by GCDO, that include Cloud services, is appended as **Appendix B**.

Through these All of Government digital contracts, agencies can consume Cloud services at their own discretion. Risk, security and other due diligence activities are the responsibility of individual agencies to ensure their unique requirements are met.

7. *Question: Are there plans to build any further dedicated government data centres in New Zealand (in addition to the one mentioned above)? And if yes, given the risk of a volcanic eruption in Auckland, have any alternative locations been discussed?*

Response: GCDO is not aware of any existing plans to build a second dedicated government Data Centre in New Zealand.

B: New Zealand Government data stored in data centres owned by overseas companies, either in New Zealand or overseas

8. *Question: Do any offshore data centres currently store New Zealand Government data? Please explain where the data centres are located and what company owns the data centre/s. NB: We understand that two Australian data centres, owned by Microsoft and Amazon respectively, did store New Zealand Government data.*

Response: Yes, offshore Data Centres do currently store New Zealand Government data; however, GCDO does not hold a list of data centre locations or their ownership.

9. *Question: Is the New Zealand Government data stored offshore 'confined' to Australian data centres? NB: We understand some global companies move data from one country to another country, depending on fluctuations in costs and volumes.*

Response: No, New Zealand Government data is not confined to Australian Data Centres and in some instances is stored globally.

Suppliers of Cloud services have mechanisms in place to ensure data and services can survive disruptions to individual data centres, including the shifting of data between Data Regions and countries. Not all Cloud services are available in New Zealand or Australian Data Centres.

With regards to All of Government digital contracts, GCDO is responsible for ensuring Data Centres meet the requirements under the New Zealand Information Security Manual (NZSIM). Outside of the All of Government digital contracts, this is the responsibility of individual agencies.

10. *Question: Is the data solely retrievable/accessible by the New Zealand Government, or does the owner of the offshore data centre (such as Microsoft and Amazon) have some ability to access the data? If yes, under what circumstances?*

Response: GCDO does not have visibility of all the Cloud services individual agencies are consuming; however, All of Government digital contracts do not allow suppliers to access encryption keys, denying them unencrypted access to New Zealand Government data.

New Zealand Government data held in offshore Data Centres is retrievable in its encrypted form by the Data Centre owner. This enables the Data Centre owner to process data effectively, but the Data Centre owner cannot see unencrypted data.

11. *Question: Are the Microsoft- and Amazon-owned data centres subject to overseas laws generally, such as the US CLOUD Act, which could mean US-owned cloud providers can be forced to hand over data to the US authorities – see [here](#)? What laws exist in New Zealand to prevent cloud providers being forced to hand over data to other countries?*

Response: Yes, New Zealand Government data is subject to the US CLOUD Act; however, there are some compensating controls such as Bring Your Own Key (BYOK) encryption. All of Government digital contracts do not allow suppliers to access encryption keys, denying them access to New Zealand Government data.

12. *Question: Can you confirm that there is a back-up system in place in case the overseas-owned data centre is attacked/compromised? Are there plans in place if the New Zealand Government is unable to access the data that is stored offshore? Please explain the system and plans.*

Response: All of Government digital contracts place requirements on Cloud suppliers to advise GCDO promptly of any such scenario, and to work with government to quickly restore services.

Agencies are individually responsible for their own Disaster Recovery and Business Continuity planning.

13. *Question: Has the New Zealand Government considered creating offshore backups in the form of a 'Data Embassy' in another country? The Estonian government has established a data embassy in Luxemburg which is fully under Estonian control and has the same rights as a physical embassy (see [here](#)).*

Response: GCD0 is aware that an offshore New Zealand Data Embassy was explored in 2015; however, was not pursued due to the high cost of such a programme.

D: Strategy

20. *Question: Work is clearly underway to make New Zealand less dependent and more resilient, but we are keen to clarify the extent we are currently vulnerable and what success might look like in the next few years. Can you provide any documents that set out New Zealand's strategy on any of the above topics?*

Response: GCD0 does not hold any information in scope of this question and therefore it is refused under section 18(e) of the Act, as the documents alleged to contain the information requested do not exist.

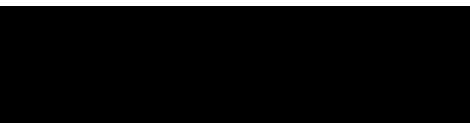
Proactive release of this response

We intend to publish our response to your request on www.dia.govt.nz. This letter, with your personal details removed, will be published in its entirety. Publishing responses increases the availability of information to the public and is consistent with the Act's purpose of enabling more effective participation in the making and administration of laws and policies and promoting the accountability of Ministers and officials.

Access to the Ombudsman

You have the right to seek an investigation and review of my decision by the Office of the Ombudsman. Information about how to make a complaint is available at www.ombudsman.parliament.nz or freephone 0800 802 602.

Nāku noa, nā



Director Ministerial and Monitoring

Appendix A: Your Official information Act 1982 request

Background

The McGuinness Institute has recently published a draft infographic, *New Zealand daily life: overseas dependencies and threats*¹. One of the dependencies identified was the storage of New Zealand Government data offshore.

We have tried to understand the current state of government data storage, but we were unable to find any definitive answers on government websites, although there has been some discussion about the risks and dependencies in the media.

Our understanding is that in 2018, the Privacy Commissioner announced that they would store their data in a Microsoft-owned data centre in Australia (see [here](#))². This 2022 article also mentions that '[m]asses of New Zealand government data is with Amazon in Sydney', and that at the time there was only one locally owned option, Catalyst Cloud. More recently, it has been in the news that both Amazon and Microsoft have been investing in data centres in New Zealand. In December 2024, a news article said that Microsoft had opened the 'first hyperscale data centre in New Zealand' (see [here](#))³, with Amazon set to launch its own Auckland-based cloud storage in 2025 (see [here](#))⁴. Last month it was in the news that GCSB and NZDF have been working on a dedicated government data centre in West Auckland 'tailor-made' for the country's most secret and sensitive public sector information (see [here](#))⁵.

Questions

This email aims to obtain more clarity over the real dependencies and threats that may exist today and how these might be managed going forward. Given this background, we have 20 questions:

A: New Zealand Government data located in data centres in New Zealand

1. Is all New Zealand Government data stored in New Zealand? What percentage of data is stored here? What percentage of agencies only store their data here.
2. Is the New Zealand Government storing data in *Microsoft's* first hyperscale data centre in New Zealand? If yes, roughly what percentage? If no, are there any plans to do so?
3. Is the New Zealand Government planning to store data at *Amazon's* new data centre in Auckland, New Zealand? If yes, roughly what percentage?
4. Is the New Zealand Government storing data with the New Zealand company *Catalyst Cloud*? Note that their website (see [here](#))⁶ states that they are an 'approved cloud provider to the New Zealand Government'. If yes, roughly what percentage of data? If no, are there any plans to do so?

¹ www.mcguinnessinstitute.org/publications/infographics

² www.rnz.co.nz/news/national/471967/head-in-the-clouds-call-for-nz-to-take-control-of-data-storage

³ www.rnz.co.nz/news/national/536389/microsoft-opens-first-hyperscale-data-centre-in-new-zealand

⁴ www.reseller.co.nz/article/3617508/aws-unveils-launch-customers-for-7-5bn-auckland-cloud-region-data-centre.html

⁵ www.rnz.co.nz/news/national/562138/formerly-secret-spy-data-centre-to-open-soon-in-west-auckland

⁶ catalystcloud.nz/

5. Can you provide a list of approved cloud providers to the New Zealand Government?
6. What is the plan for the GCSB and NZDF dedicated government data centre (mentioned above)? For example, will the new data centre store all New Zealand Government data or only a small portion (please explain roughly the percentage)? When will this new data centre be operational? Who will own the data centre? Will all data currently located offshore be removed from the overseas data centre and moved back to the new dedicated government data centre?
7. Are there plans to build any further dedicated government data centres in New Zealand (in addition to the one mentioned above)? And if yes, given the risk of a volcanic eruption in Auckland, have any alternative locations been discussed?

B: New Zealand Government data stored in data centres owned by overseas companies, either in New Zealand or overseas

These risks could take many forms, such as disrupted access due to earthquakes, cyber attacks, blackmail, or attacks by unwelcome actors.

8. Do any offshore data centres currently store New Zealand Government data? Please explain where the data centres are located and what company owns the data centre/s. NB: We understand that two Australian data centres, owned by Microsoft and Amazon respectively, did store New Zealand Government data.
9. Is the New Zealand Government data stored offshore 'confined' to Australian data centres? NB: We understand some global companies move data from one country to another country, depending on fluctuations in costs and volumes.
10. Is the data solely retrievable/accessible by the New Zealand Government, or does the owner of the offshore data centre (such as Microsoft and Amazon) have some ability to access the data? If yes, under what circumstances?
11. Are the Microsoft- and Amazon-owned data centres subject to overseas laws generally, such as the US CLOUD Act, which could mean US-owned cloud providers can be forced to hand over data to the US authorities – see [here](#)?⁷ What laws exist in New Zealand to prevent cloud providers being forced to hand over data to other countries?
12. Can you confirm that there is a back-up system in place in case the overseas-owned data centre is attacked/compromised? Are there plans in place if the New Zealand Government is unable to access the data that is stored offshore? Please explain the system and plans.
13. Has the New Zealand Government considered creating offshore backups in the form of a 'Data Embassy' in another country? The Estonian government has established a data embassy in Luxemburg which is fully under Estonian control and has the same rights as a physical embassy (see [here](#))⁸.

⁷ catalystcloud.nz/about/data-sovereignty/

⁸ e-estonia.com/solutions/e-governance/data-embassy

C: Data disruptions due to damage to our international submarine cables

These risks could take many forms, such as cables being damaged due to earthquakes, cyber attacks, blackmail, or attacks by unwelcome actors (e.g. what NATO calls ‘seabed warfare’)⁹.

14. Has a risk assessment been undertaken of disruptions to submarine cables (e.g. if an earthquake severs the undersea cables that connect New Zealand and Australia)? If yes, by whom and when?
15. Does New Zealand have all the necessary skills and resources to repair a damaged cable if 10km of cable needs to be replaced between New Zealand and Australia without help from another country? If no, do New Zealand and Australia together have the necessary skills and resources to replace 10km cables, without any external help?
16. This article¹⁰ notes, ‘Any damage could take months to repair.’ If all the skills and resources are available in New Zealand and Australia, what is the range if 10km of cable needs to be replaced (e.g. 1–3 months or 1–12 months)?
17. What is the plan B if the cables are disrupted? How would New Zealand transmit key data to the world and vice versa? Given that the volume of data is likely to be restricted during a disruption, has work been done to select what data should take precedence (e.g. financial data)?
18. What protections and/or agreements are planned/in place to secure and protect our existing cables (e.g. underwater cameras, drones etc)? Who is responsible for such plans for international submarine cables?
19. There is a number of proposed cables¹¹ that are expected to be in operation in 2026, 2027 and 2028 (e.g. the SX Tasman Express, see article)¹². Can you please list each of the existing and proposed undersea cables between Australia and New Zealand and advise who owns them? We want to understand whether New Zealand has control over the cables. Are any of the proposed cables being built or planned to be built between Australia and New Zealand owned by the New Zealand Government or in collaboration with the New Zealand Government? If yes, are they on time and within budget? Further, please indicate if the resulting capacity will include a degree of redundancy and if yes, how is that redundancy being calculated?

D: Strategy

20. Work is clearly underway to make New Zealand less dependent and more resilient, but we are keen to clarify the extent we are currently vulnerable and what success might look like in the next few years. Can you provide any documents that set out New Zealand’s strategy on any of the above topics?

⁹ www.rnz.co.nz/news/national/559165/nz-submarine-cables-are-attractive-espionage-targets-officials-warn

¹⁰ www.rnz.co.nz/news/national/559165/nz-submarine-cables-are-attractive-espionage-targets-officials-warn

¹¹ www.submarineablemap.com/country/new-zealand

¹² www.datacenterdynamics.com/en/news/southern-cross-plans-new-australia-new-zealand-subsea-cable

Appendix B: A list of organisations that hold All of Government Cloud Framework Agreements with the Government Chief Digital officer.

All of Government Digital Marketplace

The Government Chief Digital Officer’s Digital Marketplace includes a Channel for Public Cloud Services (SaaS), providing agencies with access to approved suppliers of Cloud services. A full list, and more information about Marketplace can be found at the following URL: marketplace.govt.nz/about-marketplace/whats-open-on-marketplace/approved-suppliers#Top.

All of Government Framework Agreements

The Government Chief Digital Officer also hold Cloud, and Software Framework Agreements. A full list is provided below, alongside links to more information available on Digital.govt.nz.

Cloud supplier	Contract type	URL
Amazon Web Services	Framework Agreement	www.dns.govt.nz/products-and-services/products-and-services-a-z/amazon-web-services-cloud-services-agreement-acsa
Catalyst Cloud	Framework Agreement	www.dns.govt.nz/products-and-services/products-and-services-a-z/catalyst-cloud-framework-agreement
Datacom	Framework Agreement	www.dns.govt.nz/products-and-services/products-and-services-a-z/datacom-cloud-framework-agreement
Google	Framework Agreement	www.dns.govt.nz/products-and-services/products-and-services-a-z/google-cloud-framework-agreement
Microsoft	Framework Agreement	www.dns.govt.nz/products-and-services/products-and-services-a-z/microsoft-cloud-software-and-services-agreement
SAP	Framework Agreement	www.dns.govt.nz/products-and-services/products-and-services-a-z/sap-cloud-framework-agreement
TechnologyOne	Framework Agreement	www.dns.govt.nz/products-and-services/products-and-services-a-z/technologyone-cloud-framework-agreement
Oracle	Framework Agreement	www.dns.govt.nz/products-and-services/products-and-services-a-z/oracle-software-framework-agreement

Infrastructure as a Service (IaaS) Panel

Common Capability ICT IaaS is a managed and hosted computing solution for government agencies containing 4 core services: Data Centre services, Utility Compute Services, Storage and Back-up Services.

Government Chief Digital Officer hold All of Government contracts with Datacom, Spark NZ, and T4 Group. More information can be found on Digital.govt.nz at the following URL: www.digital.govt.nz/products-and-services/products-and-services-a-z/infrastructure-as-a-service.